Exhibit 2

VISA

Visa International Operating Regulations

15 October 2012

- Issued to a commercial entity or a designated unit of the entity.

ID#: 151012-140711-0026396

Visa Central Travel Account - Issuer Liability (Updated)

All Visa Central Travel Accounts may be issued with or without a physical Card. The Issuer assumes full liability for any misuse on physical Cards issued on a Visa Central Travel Account.

ID#: 151012-140711-0026397

Visa Central Travel Account - Core Feature Requirements (Updated)

All Visa Central Travel Account Issuers must:

- Comply with the core feature requirements for the applicable product
- Provide travel accident insurance coverage when travel-related tickets are purchased using the Visa Central Travel Account. If standard policies do not include Visa Central Travel Accounts, Members must purchase coverage through Visa or another provider.
- Comply with the *Visa Commercial Format Specifications* and offer electronic management information reports at a company level detailing all spend relating to the company account on at least a monthly basis. The management information reports must include at a minimum:
  - Ticket number
  - Passenger name
  - Date of travel

ID#: 151012-140711-0026398

Visa Central Travel Account - Issuer Fees (Updated)

Visa assesses fees for all Visa Central Travel Accounts as specified in the applicable pricing guide.

ID#: 151012-140711-0026399

Visa Commercial Card Enhanced Data - Canada Region (Updated)

In the Canada Region, a Member or a Member's client participating in the Enhanced Data Service must comply with the *Visa Commercial Data Services Terms and Conditions.*

ID#: 151012-010410-0004187

Basic Currency Conversion Rate Application - CEMEA Region

In the CEMEA Region, Visa applies the Basic Currency Conversion Rate to Transaction Receipts, Credit Transaction Receipts, and Cash Disbursements. The Basic Currency Conversion Rate for Intraregional and Interregional Transactions is either the wholesale Transactions market rate or government-mandated rate in effect one day before the Central Processing Date.

The Issuer may apply an Optional Issuer Fee on the Basic Currency Conversion Rate. Visa will only apply such a fee on the Issuer's instruction.

ID#: 010410-010410-0005450

Authorization Currency - CEMEA Region

A CEMEA Member must:

- Submit Authorization Requests in the Transaction Currency
- Receive Authorization Requests in its Billing Currency

ID#: 010410-010410-0008898

ATM Clearing

ATM Cash Disbursement Transaction Classification

An ATM Cash Disbursement is a Visa Transaction if it is made with a Visa Card or Visa Electron Card.

An ATM Cash Disbursement is a Plus Transaction if it is made with a Proprietary Card bearing the Plus Symbol. A Visa Region or its exclusive Plus Program sublicensee may redefine a Plus Transaction involving a Card bearing the Plus Symbol for Intraregional Transactions.

ID#: 010410-010410-0008996

ATM Clearing Requirements

An ATM Transaction cleared through VisaNet must have been authorized through VisaNet.

ID#: 010410-010410-0004795

Global Brand Protection Program Annual Assessment Fee (Updated)

Effective 1 December 2011, an Acquirer that is subject to an annual assessment, as specified in " Annual Assessments," will be subject to an annual assessment fee, as specified in the applicable Fee Guide.

ID#: 151012-011211-0026386

Fraud Reporting

Fraud Reporting Requirements

Fraud Activity Reporting

An Issuer must report Fraud Activity to Visa through VisaNet when either a:

- Fraudulent User has obtained a Card or Account Number
- Card was obtained through misrepresentation of identification or financial status

ID#: 010410-010410-0002389

Fraud Activity Reporting Time Limit

An Issuer must report Fraud Activity upon detection, but no later than:

- 90 calendar days from the Transaction Date
- 30 calendar days following the receipt of the Cardholder's dispute notification, if the notification is not received within the 90-calendar-day period

ID#: 010410-010410-0002390

Fraud Activity Reporting Time Limit - AP Region

An AP Issuer must report all confirmed fraudulent Transactions immediately upon detection, but no later than:

- 60 calendar days from the Transaction Date
- 30 calendar days following receipt of the Cardholder's dispute notification, if the notification is not received within the 60-calendar-day period

ID#: 010410-010410-0002246

Global Compromised Account Recovery (GCAR)

Global Compromised Account Recovery Program Overview (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, an Issuer in Visa International or Visa Europe may recover a portion of its Incremental Counterfeit Fraud losses and operating expenses resulting from an Account Data Compromise Event involving a compromise of Magnetic-Stripe Data, and PIN data for events that also involve PIN compromise, under the Global Compromised Account Recovery (GCAR) program from an Acquirer(s) to whom liability for such loss has been assigned under the GCAR program.

GCAR allows Visa to determine the monetary scope of an Account Data Compromise Event, collect from the responsible Acquirer(s), and reimburse Issuers that have incurred losses as a result of the event.

GCAR allows recovery of counterfeit transaction losses across all Visa-owned brands (i.e., Visa, Interlink, Plus, and Visa Electron) when a violation, attributed to another Visa Member, could have allowed Magnetic-Stripe Data (and PIN data, if applicable) to be compromised and the subsequent financial loss was associated with **any** of the following:

- A Visa Transaction
- An Interlink transaction
- A Plus Transaction
- A Visa Electron Transaction

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, the GCAR program is only available when:

- There has been a violation involving non-compliance with one or more of the following:
  - Payment Card Industry Data Security Standard (PCI DSS)
  - PIN Management Requirements Document
  - *Visa PIN Security Program Guide*
- The violation could allow a compromise of contents of any track on the Magnetic Stripe (and PIN data, if applicable) for a Visa Transaction, a Plus Transaction, an Interlink transaction, or a Visa Electron Transaction

ID#: 151012-150512-0026564

GCAR Qualification (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will determine Account Data Compromise Event qualification, Counterfeit Fraud Recovery and Operating Expense Recovery amounts, Issuer eligibility, and Acquirer liability under the Global Compromised Account Recovery (GCAR) program, in accordance with the *Visa Global Compromised Account Recovery (GCAR) Guide*.

To qualify an Account Data Compromise Event under GCAR, Visa must determine that all of the following criteria have been met:

- A Payment Card Industry Data Security Standard (PCI DSS), PIN Management Requirements Documents, or *Visa PIN Security Program Guide* violation has occurred that could have allowed a compromise of Account Number and Card Verification Value (CVV) Magnetic-Stripe Data, and PIN data for events also involving PIN compromise
- Account Number and CVV Magnetic-Stripe Data has been exposed to a compromise
- 15,000 or more eligible accounts were sent in CAMS Internet Compromise (IC) and/or Research and Analysis (RA) alerts indicating Account Number and CVV Magnetic-Stripe Data is potentially at risk
- A combined total of US $150,000 or more Counterfeit Fraud Recovery and Operating Expense Recovery for all Issuers involved in the event
- Elevated Magnetic-Stripe counterfeit fraud was observed in the population of eligible accounts sent in the CAMS Alert(s) associated with the Account Data Compromise Event

ID#: 151012-150512-0026565

GCAR - Preliminary Determination of Event Qualification

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, following preliminary fraud analysis and investigation of an Account Data Compromise Event, Visa will provide the Acquirer(s) with:

- Findings in support of the preliminary determination that the event is qualified for the Global Compromised Account Recovery (GCAR) program
- A preliminary estimate of counterfeit fraud and operating expense liability amounts

ID#: 160312-150512-0026566

GCAR - Appeal Rights

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, an Acquirer may appeal a Global Compromised Account Recovery (GCAR) preliminary determination of Account Data Compromise Event qualification to Visa by submitting an appeal letter. The appeal letter must:

- Be received by Visa within 30 calendar days of the Acquirer's receipt of the preliminary Notification of qualification and estimated liability
- Include written arguments and supporting information for the appeal

Visa will notify the Acquirer of the final disposition of the appeal. The decision on the appeal is final and not subject to any challenge or any other appeal rights.

The appeal rights as specified in "Enforcement Appeals" are not applicable to GCAR.

ID#: 160312-150512-0026567

GCAR - Appeal Fee (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will collect from the Acquirer through the Global Member Billing System a Global Compromised Account Recovery (GCAR) appeal fee, as specified in the applicable Fee Guide.

ID#: 151012-150512-0026568

GCAR - Notification of Final Liability and Recovery Amounts

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will notify the Acquirer(s) deemed responsible for an Account Data Compromise Event of its final counterfeit fraud and operating expense liability amounts under Global Compromised Account Recovery (GCAR).

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will notify the affected Issuers that an Account Data Compromise Event qualifies for Operating Expense Recovery and Counterfeit Fraud Recovery under GCAR, and advise them of their recovery amounts.

ID#: 160312-150512-0026569

GCAR - Debits, Credits, and Fees (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will submit debits to the Acquirer(s) responsible for an Account Data Compromise Event and credits, less administrative fees, to eligible Issuers through the Global Member Billing System. Visa retains a Global Compromised Account Recovery (GCAR) program administration fee, as specified in the applicable Fee Guide. The debit and credit amounts as determined by Visa are final and not subject to any appeal or other challenge.

ID#: 151012-150512-0026570

GCAR - Non-Cooperation Analysis Fee (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa assesses to the Acquirer through the Global Member Billing Systems, a Global Compromised Account Recovery (GCAR) program non-cooperation analysis fee, as specified in the applicable Fee Guide, if the Acquirer, its Merchant, or other Compromised Entity refuses to allow a forensics investigation.

ID#: 151012-150512-0026571

GCAR - Conditions for Reimbursement

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, reimbursements under the Global Compromised Account Recovery (GCAR) program to affected Issuers are based solely upon the ability of Visa to collect the counterfeit fraud and operating expense liability amounts from the responsible Acquirer(s).

ID#: 160312-150512-0026572

GCAR - Catastrophic Loss

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, if an Account Data Compromise Event is deemed catastrophic, Visa reserves the right to implement an alternative process to the Global Compromised Account Recovery (GCAR) program.

ID#: 160312-150512-0026573

GCAR Program Compliance (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, a Member must comply with the *Visa Global Compromised Account Recovery (GCAR) Guide*.

ID#: 151012-150512-0026749

GCAR Incremental Fraud Recovery

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, to determine Incremental Fraud Recovery, the Global Compromised Account Recovery (GCAR) program:

- Uses an Incremental Counterfeit Fraud calculation that is based on actual counterfeit fraud reported in excess of the Issuer's baseline counterfeit fraud during an alert's Fraud Window. The Issuer baseline is determined at the BIN level and calculated for each alert based on a set methodology.

- Uses an Issuer Counterfeit Fraud Recovery limit to incent effective management of fraud. Issuer counterfeit fraud reported in excess of US $3,000 per account will be excluded from Incremental Counterfeit Fraud recovery calculations.
- Excludes from the Issuer recovery calculation Transactions that have been successfully charged back by the Issuer and for which the Acquirer has not submitted a successful Representment at the time of the calculation
- Includes in the Issuer recovery calculation fraud Transactions that occurred up to 12 months prior to and one month following the CAMS date

Counterfeit fraud Transactions must have been authorized through VisaNet to be eligible for GCAR recovery. The only exception to this rule is that on-us [126] ATM counterfeit fraud Transactions on Plus accounts will be eligible for GCAR recovery if the Issuer is in a country where at least 95% of domestic volume of Visa-owned brands (excluding on-us ATM) is authorized through VisaNet.

ID#: 160312-150512-0026751

GCAR Operating Expense Recovery

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Operating Expense Recovery under the Global Compromised Account Recovery (GCAR) program is US $2.50 per eligible account on Internet Compromise (IC) and/or Research and Analysis (RA) CAMS-alerted accounts that were not identified as expired at the time of the CAMS Alert.

ID#: 160312-150512-0026752

GCAR General Calculation Rules

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, the following general rules are applicable for Global Compromised Account Recovery (GCAR) calculations:

- Issuers must use CAMS to be eligible for recovery
- Accounts must have been authorized through VisaNet in a Transaction processed through the Compromised Entity during the Account Data Compromise Event timeframe to be included in Acquirer liability and Issuer recovery calculations
- Accounts included in a different CAMS Alert in the prior 12 months are excluded from the Acquirer liability and Issuer recovery calculations
- Visa reserves the right to adjust an Acquirer's total liability for an Account Data Compromise Event

ID#: 160312-150512-0026753

126 An On-Us Transaction is a Transaction where the Issuer and the Acquirer are the same Member.

Chapter 10: Pricing, Fees and Interchange

Core Principle 10.1

Fees for Access and Use of Visa Products and Services

Establishing Fees for Access

Visa system participants pay fees to Visa for access to and use of Visa products and services. Visa establishes certain fees between issuers and acquirers for specific participant actions such as rewards paid to store clerks for card recovery or the fulfillment of sales receipt copies.

ID#: 010410-010410-0007825

Core Principle 10.2

Participants Pay or Receive Interchange for Transactions

Paying or Receiving Interchange

Participating acquirers and issuers pay or receive interchange every time a Visa product is used. For example, acquirers pay interchange to issuers for purchase transactions and issuers pay interchange to acquirers for cash transactions and credit vouchers. In the case of a credit or a chargeback, interchange flows in reverse.

ID#: 010410-010410-0007826

What is Interchange?

Interchange reimbursement fees help to make electronic payments possible by enabling Visa to expand card holding and use, increasing the places consumers can use their cards and providing a financial incentive for all parties to pursue system-wide improvements, such as rewards, innovation and security. An interchange reimbursement fee is a default transfer price between acquirers and issuers within the Visa system. Merchants pay what is known as a merchant discount fee or merchant service fee negotiated with their acquirer which may take into account the interchange fee, processing costs, fees for terminal rental, customer services, and other financial services. The merchant discount fee or merchant service fee is negotiated individually with the merchant's acquirer; each acquirer sets its fees independently, in competition with other acquirers, competing payment systems, and other forms of payment.

Interchange is consistently monitored and adjusted - sometimes increased and sometimes decreased - in order to ensure that the economics present a competitive value proposition for all parties. Interchange reimbursement fees must encourage card holding and use, as well as expansion in the number and types of businesses that accept cards. If rates are too high, retailers won't accept cards; if rates are too low, issuers won't issue cards. Visa may establish different interchange reimbursement fees in order to promote a variety of system objectives, such as enhancing the value proposition for Visa products, providing incentives to grow merchant acceptance and usage, and reinforcing strong system security and transaction authorization practices.

ID#: 010410-010410-0024115

Core Principle 10.3

Visa Determines Interchange Reimbursement Fees

Visa Determines and Publishes IRF

Interchange reimbursement fees are determined by Visa and provided on Visa's published fee schedule, or may be customized where members have set their own financial terms for the interchange of a Visa transaction or Visa has entered into business agreements to promote acceptance and card usage.

ID#: 010410-080210-0024122

Global Interchange

Interchange Overview

Interchange Reimbursement Fee Rate Sheets and Guides

The Interchange Reimbursement Fee (IRF) is based on several factors. These primarily include Card type, Merchant type, and Transaction type. Interchange Reimbursement Fee rates are available to Members through regional online resources or Visa account executives. Interchange requirements are contained in the *Visa International Operating Regulations* and the applicable domestic or regional Interchange Qualification Guide. In addition, there are many other types of Visa transactions, such as Original Credits, ATM inquiries, etc., that are detailed in the Operating Regulations.

ID#: 010410-010410-0006577

3-D Secure Specification - U.S. Region

Effective through 14 March 2012, a software protocol that enables secure processing of Transactions over the Internet and other networks.

ID#: 160312-010410-0024204

A

Acceptance Mark - U.S. Region

A Visa-Owned Mark that denotes Point-of-Transaction acceptance for payments and Cash Disbursements under specific rules.

ID#: 150511-010410-0024205

Access Control Server - U.S. Region

Effective through 14 March 2012, a component of the 3-D Secure Authenticated Payment Program that provides functionality for authentication, attempted authentication, and related Authentication Record messaging, as specified in the *3-D Secure Issuer Implementation Guide.*

ID#: 160312-010410-0024206

Access Fee

A fee that is imposed by an ATM Acquirer as part of a Cash Disbursement Transaction, to a Cardholder for use of its ATM.

ID#: 150511-180409-0024207

Account Data Compromise Event

An event in which a security breach puts account data at risk of being stolen.

ID#: 160312-150512-0026743

Account Data Compromise Recovery Process - U.S. Region

Effective through 14 May 2012, a Visa-initiated process to facilitate allocation of liability between Members for certain losses incurred as the result of an account compromise event.

ID#: 160312-010410-0024212